Sub A1

What is claimed is:

1. A public key authentication system for use in a computer system having a plurality of users, the system comprising:

a virtual smart card server;

storage connected to the virtual smart card server, wherein the storage includes a plurality of virtual smart cards, wherein each virtual smart card is associated with a user and wherein each smart card includes a private key; and

a virtual smart card agent connected to the virtual smart card server, wherein the virtual smart card agent authenticates the user and accesses the authenticated user's virtual smart card to obtain the user's private key.

2. The public key authentication system according to claim 1, wherein the virtual smart card agent includes an interface to a smart-card-enabled application.

3. The public key authentication system according to claim 2, wherein the virtual smart card server performs encryption in response to a remote call from the interface.

4. The public key authentication system according to claim 2, wherein the virtual smart card server performs signing in response to a remote call from the interface.

5. The public key authentication system according to claim 2, wherein the virtual smart card server performs key management functions in response to a remote call from the interface.

6. The public key authentication system according to claim 1, wherein the public key authentication system further includes an authentication server connected to the virtual smart card agent and wherein the virtual smart card agent authenticates the user through interaction with the authentication server.

7. The public key authentication system according to claim 1, wherein the public key authentication system further includes an authentication server connected to the virtual smart card server and wherein the virtual smart card agent authenticates the user through interaction with the authentication server.

8. The public key authentication system according to claim 1, wherein the virtual smart card agent communicates with the virtual smart card server over an agent-server transport layer.

9. The public key authentication system according to claim 1, wherein the virtual smart card agent communicates with the virtual smart card server over a secure TCP/IP session.

10. A method of authenticating users, including a first user, attempting to access a computer system, the method comprising:

assigning first and second keys to each user, wherein the first and second key form a public/private key pair;

issuing a digital certificate to the first user, wherein the digital certificate is associated with the second key assigned to the first user;

entering a one-time password;

encrypting the one-time password with the first key assigned to the first user to form an encrypted one-time password;

verifying that the digital certificate issued to the first user was signed by a recognized certificate authority;

accessing, via the digital certificate, the second key assigned to the first user;

decrypting the encrypted one-time password with the second key associated with the digital certificate to recover the one-time password; and

comparing the one-time password against an expected one-time password.

11. The method according to claim 10, wherein the first key is a private key and the second key is a public key.

12. The method according to claim 10, wherein verifying that the digital certificate issued to the first user was signed by a recognized certificate authority includes accessing a CRL to determine if the certificate has been revoked.

13. A computer-readable medium comprising program code which executes the method of claim 10.

14. A public key authentication system for use in a computer system having a plurality of users, the system comprising:

an authentication server;

a directory service connected to the authentication server, wherein the directory service includes a plurality of public keys, wherein each public key is associated with a unique user identifier; and

a host system, wherein the host system includes a public key authentication client and an interface to a smart-card-enabled application, wherein the public key authentication client is connected to the authentication server;

wherein the public key authentication client receives a challenge issued by the authentication server, signs the challenge with a digital signature representing a user and sends the digital signature of the challenge back to the authentication server; and

wherein the authentication server receives the digital signature of the challenge and verifies the digital signature with a public key retrieved from the directory service.

15. The public key authentication system according to claim 14, wherein the authentication server includes role-based access control.

16. The public key authentication system according to claim 14, wherein the authentication server includes automatic logging of authentication attempts.